

**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently amended) An information processing system comprising:  
a first information processing apparatus and a second information processing apparatus, the first information processing apparatus comprising  
an interface having an isochronous transmission mode in which a transmission band is ensured, and  
a transmission control means for controlling encrypted data in the transmission band,  
wherein the encrypted data is encrypted using an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number, and then the encrypted data is transmitted in the isochronous transmission mode via the interface,  
wherein the transmission control means executes, prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys with the second information processing apparatus, to which the encrypted data is to be transmitted, and from which an authentication request is to be received, and  
wherein the first information processing apparatus encrypts the data following said authentication request from the second information processing apparatus; and  
the second information processing apparatus comprising

an interface having the isochronous transmission mode in which a transmission band is ensured, and

a receiving control means for controlling reception of encrypted data received by the second information processing apparatus from the first information processing apparatus,

wherein the encrypted data which is received in the isochronous transmission mode via the interface is decrypted using the encryption key,

wherein the receiving control means executes, prior to data reception, a protocol for performing mutual authentication and sharing a plurality of encryption keys with the first information processing apparatus, from which the encrypted data is to be received, and to which an authentication request is to be transmitted, and

wherein the second information processing apparatus ~~decodes~~ decrypts the encrypted data following an authentication request to the first information processing apparatus.

2. (Canceled)

3. (Canceled)

4. (Original) The information processing system as claimed in claim 1, wherein the first information processing apparatus and the second information processing apparatus are connected with each other via an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, for transmitting data

requiring the assurance of a transmission band in an isochronous transmission mode and for transmitting related data relating to the data in an asynchronous transmission mode.

5. (Canceled)

6. (Previously presented) The information processing system as claimed in claim 1, wherein the second information processing apparatus generates two random numbers and transmits them to the first information processing apparatus,

the first information processing apparatus generates two random numbers and transmits them to the second information processing apparatus,

the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting data to be transmitted in a second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number, and

the second information processing apparatus generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number.

7. (Previously presented) The information processing system as claimed in claim 6, wherein the first information processing apparatus transmits data P generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the first information processing apparatus,

the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data Q, and

the second information processing apparatus generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data P.

8. (Previously presented) The information processing system as claimed in claim 7, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus,

the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus,

the first information processing apparatus transmits data P generated on the basis of information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus,

the first information processing apparatus generates an encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and

the second information processing apparatus generates an encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and an encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the

validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

9. (Previously presented) The information processing system as claimed in claim 8, wherein the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2.

10. (Previously presented) The information processing system as claimed in claim 9, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the second information processing apparatus,

the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

11. (Original) The information processing system as claimed in claim 9, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function.

12. (Original) The information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function.

13. (Original) The information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a least significant n bits of the result of calculation of the unidirectional function.

14. (Original) The information processing system as claimed in claim 13, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a most significant m bits of the result of calculation of the unidirectional function.



15. (Previously presented) The information processing system as claimed in claim 8, wherein the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2.

16. (Previously presented) The information processing system as claimed in claim 15, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus,

the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a

unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

17. (Previously presented) The information processing system as claimed in claim 6, wherein the first information processing apparatus and the second information processing apparatus generate either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, and generate the encryption key of the other transmission mode on the basis of the generated encryption key, the generated random number and the received random number.

18. (Previously presented) The information processing system as claimed in claim 17, wherein the first information processing apparatus generates either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, and transmits data P generated on the basis of the generated encryption key, the received random number and the generated random number to the second information processing apparatus,

the second information processing apparatus generates either one of the encryption key used for decrypting the data transmitted in the isochronous transmission mode and the encryption key used for decrypting the data transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, and verifies whether or not data P' generated on the basis of the generated encryption key, the received random number and the generated random number is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number to the first information processing apparatus and generates the encryption key of the transmission mode for which the encryption key is not generated yet, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key of the transmission mode for which the encryption key is already generated, the received random number and the generated random number, and

the first information processing apparatus generates the encryption key of the transmission mode for which the encryption key is not yet generated, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key of the transmission mode for which the encryption key is already generated, the received random number and the generated random number, in the case where data Q' generated on the basis of

the information indicating the validity of the apparatus itself, the received random number and the generated random number is coincident with the received data Q.

19. (Previously presented) The information processing system as claimed in claim 18, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus,

the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus,

the first information processing apparatus generates one encryption key K1 of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1, and transmits data P generated on the basis of the generated encryption key K1, the received random number R1 and the generated random number S2 to the second information processing apparatus,

the second information processing apparatus generates one encryption key K'1 of the encryption key used for decrypting the data transmitted in the isochronous transmission mode and the encryption key used for decrypting the data transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and verifies whether or not data P' generated on the basis of the generated encryption key K'1, the received random number S2 and the generated random number

R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the first information processing apparatus and generates the encryption key K'2 of the transmission mode for which the encryption key is not generated yet, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key K'1 of the transmission mode for which the encryption key is already generated, the received random number S2 and the generated random number R2, and the first information processing apparatus generates the encryption key K2 of the transmission mode for which the encryption key is not yet generated, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key K1 of the transmission mode for which the encryption key is already generated, the received random number R2 and the generated random number S2, in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1 is coincident with the received data Q.

20. (Original) The information processing system as claimed in claim 19, wherein the first information processing apparatus generates the encryption key K1 on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number R1 and the generated

random number S1, and generates the encryption key K2 on the basis of the result of calculation of a unidirectional function using the generated encryption key K1, the received random number R2 and the generated random number S2, and

the second information processing apparatus generates the encryption key K'1 on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 on the basis of the result of calculation of a unidirectional function using the generated encryption key K'1, the received random number S2 and the generated random number R2.

21. (Original) The information processing system as claimed in claim 20, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of the unidirectional function using the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus,

the second information apparatus verifies whether or not data P' generated on the basis of the result of calculation of the unidirectional function using the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the first information processing apparatus, and

the first information processing apparatus generates the encryption key K2 in the case where data Q' generated on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1 is coincident with the received data Q.

22. (Original) The information processing system as claimed in claim 20, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function.

23. (Original) The information processing system as claimed in claim 22, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function.

24. (Original) The information processing system as claimed in claim 22, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using the least significant n bits of the result of calculation of the unidirectional function.



25. (Original) The information processing system as claimed in claim 24, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using the most significant m bits of the result of calculation of the unidirectional function.

26. (Original) The information processing system as claimed in claim 19, wherein the first information processing apparatus generates the encryption key K1 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number, and generates the encryption key K2 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the generated encryption key K1, the received random number R2 and the generated random number S2, and

the second information processing apparatus generates the encryption key K'1 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K'1, the received random number S2 and the generated random number R2.

27. (Original) The information processing system as claimed in claim 26, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus,

the second information apparatus verifies whether or not data P' generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the first information processing apparatus, and

the first information processing apparatus generates the encryption key K2 in the case where data Q' generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1 is coincident with the received data Q.

28. (Currently amended) An information processing method for performing data transmission between a first information processing apparatus and a second information

processing apparatus via an interface having an isochronous transmission mode in which a transmission band is ensured, the method comprising the steps of:

encrypting data from the first information processing apparatus using an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number, and then transmitting the encrypted data in the isochronous transmission mode; and

decrypting, using the encryption key on the side of the second information processing apparatus, the encrypted data which is received in the isochronous transmission mode.

29. (Canceled)

30. (Canceled)

31. (Original) The information processing method as claimed in claim 28, wherein the first information processing apparatus and the second information processing apparatus are connected with each other via an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, for transmitting data requiring the assurance of a transmission band in an isochronous transmission mode and for transmitting related data relating to the data in an asynchronous transmission mode.

32. (Canceled)

33. (Previously presented) The information processing method as claimed in claim 28, wherein the second information processing apparatus generates two random numbers and transmits them to the first information processing apparatus,

the first information processing apparatus generates two random numbers and transmits them to the second information processing apparatus,

the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting data to be transmitted in a second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number, and

the second information processing apparatus generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number.

34. (Previously presented) The information processing method as claimed in claim 33, wherein the first information processing apparatus transmits data P generated on the basis of the information indicating the validity of the apparatus itself, the

generated random number and the received random number, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the first information processing apparatus,

the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data Q, and

the second information processing apparatus generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data P.

35. (Previously presented) The information processing method as claimed in claim 34, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus,

the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus,

the first information processing apparatus transmits data P generated on the basis of information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus,

the first information processing apparatus generates an encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and

the second information processing apparatus generates an encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and an encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

36. (Previously presented) The information processing method as claimed in claim 35, wherein the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2.

37. (Previously presented) The information processing method as claimed in claim 36, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function using the information

indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus,

the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number P2 is coincident with the received data P.

38. (Original) The information processing method as claimed in claim 36, wherein the first information processing apparatus and the second information processing



apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function.

39. (Original) The information processing method as claimed in claim 38, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function.

40. (Original) The information processing method as claimed in claim 38, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K2, using the least significant n bits of the result of calculation of the unidirectional function.

41. (Original) The information processing method as claimed in claim 40, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using the most significant m bits of the result of calculation of the unidirectional function.

42. (Previously presented) The information processing method as claimed in claim 35, wherein the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission

mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2.

43. (Previously presented) The information processing method as claimed in claim 42, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the

apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus,

the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus,

the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and

the second information processing apparatus generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

44. (Previously presented) The information processing method as claimed in claim 33, wherein the first information processing apparatus and the second information processing apparatus generate either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, and generate the encryption key of the other transmission mode on the basis of the generated encryption key, the generated random number and the received random number.

45. (Previously presented) The information processing method as claimed in claim 44, wherein the first information processing apparatus generates either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, and transmits data P generated on the basis of the generated encryption key, the received random number and the generated random number to the second information processing apparatus,

the second information processing apparatus generates either one of the encryption key used for decrypting the data transmitted in the isochronous transmission mode and the encryption key used for decrypting the data transmitted in the second transmission mode, on the basis of the information indicating the validity of the

apparatus itself, the received random number and the generated random number, and verifies whether or not data P' generated on the basis of the generated encryption key, the received random number and the generated random number is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number to the first information processing apparatus and generates the encryption key of the transmission mode for which the encryption key is not generated yet, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key of the transmission mode for which the encryption key is already generated, the received random number and the generated random number, and

the first information processing apparatus generates the encryption key of the transmission mode for which the encryption key is not yet generated, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key of the transmission mode for which the encryption key is already generated, the received random number and the generated random number, in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number is coincident with the received data Q.

46. (Previously presented) The information processing method as claimed in claim 45, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus,

the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus,

the first information processing apparatus generates one encryption key K1 of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1, and transmits data P generated on the basis of the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus,

the second information processing apparatus generates one encryption key K'1 of the encryption key used for decrypting the data transmitted in the isochronous transmission mode and the encryption key used for decrypting the data transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and verifies whether or not data P' generated on the basis of the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the received random number S1 and the

generated random number R1 to the first information processing apparatus and generates the encryption key K'2 of the transmission mode for which the encryption key is not generated yet, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key K'1 of the transmission mode for which the encryption key is already generated, the received random number S2 and the generated random number R2, and the first information processing apparatus generates the encryption key K2 of the transmission mode for which the encryption key is not yet generated, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key K1 of the transmission mode for which the encryption key is already generated, the received random number R2 and the generated random number S2, in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1 is coincident with the received data Q.

47. (Original) The information processing method as claimed in claim 46, wherein the first information processing apparatus generates the encryption key K1 on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1, and generates the encryption key K2 on the basis of the result of calculation of a unidirectional function using the generated encryption key K1, the received random number R2 and the generated random number S2, and

the second information processing apparatus generates the encryption key  $K'1$  on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number  $S1$  and the generated random number  $R1$ , and generates the encryption key  $K'2$  on the basis of the result of calculation of a unidirectional function using the generated encryption key  $K'1$ , the received random number  $S2$  and the generated random number  $R2$ .

48. (Original) The information processing method as claimed in claim 47, wherein the first information processing apparatus transmits data  $P$  generated on the basis of the result of calculation of the unidirectional function using the generated encryption key  $K1$ , the received random number  $R2$  and the generated random number  $S2$  to the second information processing apparatus,

the second information apparatus verifies whether or not data  $P'$  generated on the basis of the result of calculation of the unidirectional function using the generated encryption key  $K'1$ , the received random number  $S2$  and the generated random number  $R2$  is coincident with the received data  $P$ , and in the case where the data  $P'$  is coincident with the data  $P$ , transmits data  $Q$  generated on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself, the received random number  $S1$  and the generated random number  $R1$  to the first information processing apparatus, and

the first information processing apparatus generates the encryption key  $K2$  in the case where data  $Q'$  generated on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself,



the received random number R1 and the generated random number S1 is coincident with the received data Q.

49. (Original) The information processing method as claimed in claim 47, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function.

50. (Original) The information processing method as claimed in claim 49, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function.

51. (Original) The information processing method as claimed in claim 49, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using the least significant n bits of the result of calculation of the unidirectional function.

52. (Original) The information processing method as claimed in claim 51, wherein the first information processing apparatus and the second information processing

apparatus generate the data P, the data Q', the data Q and the data P', using the most significant m bits of the result of calculation of the unidirectional function.

53. (Original) The information processing method as claimed in claim 46, wherein the first information processing apparatus generates the encryption key K1 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number, and generates the encryption key K2 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the generated encryption key K1, the received random number R2 and the generated random number S2, and

the second information processing apparatus generates the encryption key K'1 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K'1, the received random number S2 and the generated random number R2.

54. (Original) The information processing method as claimed in claim 53, wherein the first information processing apparatus transmits data P generated on the basis of

the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus,

the second information apparatus verifies whether or not data P' generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the first information processing apparatus, and

the first information processing apparatus generates the encryption key K2 in the case where data Q' generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1 is coincident with the received data Q.

55. (Currently amended) A first information processing apparatus comprising:  
an interface having an isochronous transmission mode; and  
a transmission control means for controlling encrypted transmissions from the apparatus,

wherein data requiring the assurance of the transmission band is encrypted using an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by a second information processing apparatus, the second random number being different from the first random number, and then the encrypted data is transmitted in the isochronous transmission mode via the interface, and

wherein the transmission control means executes, prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys with the second information processing apparatus to which the encrypted data is to be transmitted, and from which an authentication request is to be received, and

wherein the first information processing apparatus encrypts the data following said authentication request from the second information processing apparatus.

56. (Canceled)

57. (Canceled)

58. (Previously presented) The first information processing apparatus as claimed in claim 55, further comprising, as the interface, an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, wherein the transmission control means transmits data requiring the assurance of a transmission band in an isochronous transmission mode and transmits related data relating to the data in an asynchronous transmission mode.

59. (Canceled)

60. (Previously presented) The first information processing apparatus as claimed in claim 55, wherein the transmission control means generates two random numbers and transmits them to the second information processing apparatus, then receives two random numbers generated by the second information processing apparatus, and generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number.

61. (Previously presented) The first information processing apparatus as claimed in claim 60, wherein the transmission control means transmits data P generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the second information processing apparatus, then receives data Q generated by the second information processing apparatus on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, and generates an encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of

the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data Q.

62. (Previously presented) The first information processing apparatus as claimed in claim 61, wherein the transmission control means receives a random number R2 generated by the second information processing apparatus, generates two random numbers S1 and S2 and transmits them to the second information processing apparatus, transmits data P generated on the basis of information indicating the validity of the apparatus itself, the generated random number S2 and the received random number P2 to the second information processing apparatus, receives data Q generated by the second information processing apparatus on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates an encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and an encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q.

63. (Previously presented) The first information processing apparatus as claimed in claim 62, wherein the transmission control means generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information

indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2.

64. (Previously presented) The first information processing apparatus as claimed in claim 63, wherein the transmission control means transmits data P generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2 to the second information processing apparatus, receives data Q generated by the second information processing apparatus on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number Si and the received random number R1 is coincident with the received data Q.

65. (Previously presented) The first information processing apparatus as claimed in claim 63, wherein the transmission control means generates the encryption key K1 and the encryption key K2, using a bit value of a part of the result of calculation of the unidirectional function.

66. (Previously presented) The first information processing apparatus as claimed in claim 65, wherein the transmission control means generates the data P and the data Q', using a bit value of a part of the result of calculation of the unidirectional function.

67. (Previously presented) The first information processing apparatus as claimed in claim 65, wherein the transmission control means generates the encryption key K1 and the encryption key K2, using the least significant n bits of the result of calculation of the unidirectional function.

68. (Previously presented) The first information processing apparatus as claimed in claim 67, wherein the transmission control means generates the data P and the data Q', using the most significant m bits of the result of calculation of the unidirectional function.

69. (Previously presented) The first information processing apparatus as claimed in claim 62, wherein the transmission control means generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function with respect to



concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2.

70. (Previously presented) The first information processing apparatus as claimed in claim 69, wherein the transmission control means transmits data P generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus, receives data Q generated by the second information processing apparatus on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K1 used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the

generated random number S1 and the received random number R1 is coincident with the received data Q.

71. (Previously presented) The first information processing apparatus as claimed in claim 60, wherein the transmission control means generates either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, and generates the encryption key of the other transmission mode on the basis of the generated encryption key, the generated random number and the received random number.

72. (Previously presented) The first information processing apparatus as claimed in claim 71, wherein the transmission control means generates either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, transmits data P generated on the basis of the generated encryption key, the received random number and the generated random number to the second information processing apparatus, receives data Q generated by the second information processing apparatus on the basis of the information indicating the validity of the

apparatus itself, the received random number and the generated random number, and generates the encryption key of the transmission mode for which the encryption key is not yet generated, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key of the transmission mode for which the encryption key is already generated, the received random number and the generated random number, in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number is coincident with the received data Q.

73. (Previously presented) The first information processing apparatus as claimed in claim 72, wherein the transmission control means receives two random numbers R1 and P2 generated by the second information processing apparatus, generates two random numbers S1 and S2 and transmits them to the second information processing apparatus, generates one encryption key K1 of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1, transmits data P generated on the basis of the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus, receives data Q generated by the second information processing apparatus on the basis of the information indicating the validity of the apparatus itself, the received

random number S1 and the generated random number R1, and generates the encryption key K2 of the transmission mode for which the encryption key is not yet generated, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key K1 of the transmission mode for which the encryption key is already generated, the received random number R2 and the generated random number S2, in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the received random number R2 and the generated random number S2 is coincident with the received data Q.

74. (Previously presented) The first information processing apparatus as claimed in claim 73, wherein the transmission control means generates the encryption key K1 on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1, and generates the encryption key K2 on the basis of the result of calculation of a unidirectional function using the generated encryption key K1, the received random number R2 and the generated random number S2.

75. (Previously presented) The first information processing apparatus as claimed in claim 74, wherein the transmission control means transmits data P generated on the basis of the result of calculation of the unidirectional function using the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus, receives data Q generated by the

other information processing apparatus on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself, the received random number  $S_i$  and the generated random number  $R_1$ , and generates the encryption key  $K_2$  in the case where data  $Q'$  generated on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself, the received random number  $R_1$  and the generated random number  $S_1$  is coincident with the received data  $Q$ .

76. (Previously presented) The first information processing apparatus as claimed in claim 74, wherein the transmission control means generates the encryption key  $K_1$  and the encryption key  $K_2$ , using a bit value of a part of the result of calculation of the unidirectional function.

77. (Previously presented) The first information processing apparatus as claimed in claim 76, wherein the transmission control means generates the data  $P$  and the data  $Q'$ , using a bit value of a part of the result of calculation of the unidirectional function.

78. (Previously presented) The first information processing apparatus as claimed in claim 76, wherein the transmission control means generates the encryption key  $K_1$  and the encryption key  $K_2$ , using the least significant  $n$  bits of the result of calculation of the unidirectional function.

79. (Previously presented) The first information processing apparatus as claimed in claim 78, wherein the transmission control means generates the data P and the data Q', using the most significant m bits of the result of calculation of the unidirectional function.

80. (Previously presented) The first information processing apparatus as claimed in claim 73, wherein the transmission control means generates the encryption key K1 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number, and generates the encryption key K2 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the generated encryption key K1, the received random number R1 and the generated random number S2.

81. (Previously presented) The first information processing apparatus as claimed in claim 80, wherein the transmission control means transmits data P generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K1, the received random number R2 and the generated random number S2 to the second information processing apparatus, receives data Q generated by the second information processing apparatus on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information

indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K2 in the case where data Q' generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1 is coincident with the received data Q.

82. (Currently amended) A first information processing apparatus comprising:  
an interface having an isochronous transmission mode in which a transmission band is ensured; and  
a receiving control means for controlling reception of encrypted data received by the apparatus from a second information processing apparatus,  
wherein the encrypted data which is received in the isochronous transmission mode via the interface is decrypted by an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number, and  
wherein the receiving control means executes, prior to data reception, a protocol for performing mutual authentication and sharing a plurality of encryption keys with the second information processing apparatus from which the encrypted data is to be received, and to which an authentication request is to be transmitted, and

wherein the first information processing apparatus ~~decodes~~ decrypts the encrypted data following said authentication request to the second information processing apparatus.

83. (Canceled)

84. (Canceled)

85. (Previously presented) The first information processing apparatus as claimed in claim 82, further comprising, as the interface, an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, wherein the receiving control means receives data requiring the assurance of a transmission band in an isochronous transmission mode and receives related data relating to the data in an asynchronous transmission mode.

86. (Canceled)

87. (Previously presented) The first information processing apparatus as claimed in claim 82, wherein the receiving control means generates two random numbers and transmits them to the second information processing apparatus, receives two random numbers generated by the second information processing apparatus, and generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second



transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number.

88. (Previously presented) The first information processing apparatus as claimed in claim 87, wherein the receiving control means receives data P generated by the second information processing apparatus on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number,

transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number to the second information processing apparatus, and generates an encryption key used for decrypting the data transmitted in the isochronous transmission mode and an encryption key used for decrypting the data transmitted in the second transmission mode in the case where data P generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data P.

89. (Previously presented) The first information processing apparatus as claimed in claim 88, wherein the receiving control means generates two random numbers R1 and R2 and transmits them to the second information processing apparatus, receives two random numbers S1 and S2 generated by the second information processing apparatus, receives data P generated by the second information processing apparatus on the basis of information indicating the validity of the apparatus itself, the generated

random number S2 and the received random number R2, transmits data Q generated on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the second information processing apparatus, and generates an encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and an encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

90. (Previously presented) The first information processing apparatus as claimed in claim 89, wherein the receiving control means generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2.

91. (Previously presented) The first information processing apparatus as claimed in claim 90, wherein the receiving control means receives data P generated by the second information processing apparatus on the basis of the result of calculation of a

unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, transmits data Q generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number Si and the generated random number R1 to the second information processing apparatus, and generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

92. (Previously presented) The first information processing apparatus as claimed in claim 90, wherein the receiving control means generates the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function.

93. (Previously presented) The first information processing apparatus as claimed in claim 92, wherein the receiving control means generates the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function.

94. (Previously presented) The first information processing apparatus as claimed in claim 92, wherein the receiving control means generates the encryption key K'1 and the encryption key K'2, using the least significant n bits of the result of calculation of the unidirectional function.

95. (Previously presented) The first information processing apparatus as claimed in claim 94, wherein the receiving control means generates the data Q and the data P', using the most significant m bits of the result of calculation of the unidirectional function.

96. (Previously presented) The first information processing apparatus as claimed in claim 89, wherein the receiving control means generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decrypting the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R1.

97. (Previously presented) The first information processing apparatus as claimed in claim 96, wherein the receiving control means receives data P generated by the

second information processing apparatus on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R1, transmits data Q generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the second information processing apparatus, and generates the encryption key K'1 used for decrypting the data transmitted in the isochronous transmission mode and the encryption key K'2 used for decrypting the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P.

98. (Previously presented) The first information processing apparatus as claimed in claim 87, wherein the receiving control means generates either one of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, receives data P generated by the second information processing apparatus on the basis of the generated encryption key, the received random number and the generated

random number, generates either one of the encryption key used for decrypting the data transmitted in the isochronous transmission mode and the encryption key used for decrypting the data transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number, verifies whether or not data P' generated on the basis of the generated encryption key, the received random number and the generated random number is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the received random number and the generated random number to the second information processing apparatus and generates the encryption key of the transmission mode for which the encryption key is not generated yet, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key of the transmission mode for which the encryption key is already generated, the received random number and the generated random number.

99. (Previously presented) The first information processing apparatus as claimed in claim 98, wherein the receiving control means generates two random numbers R1 and R2 and transmits them to the second information processing apparatus, receives two random numbers S1 and S2 generated by the second information processing apparatus, the second information processing apparatus generating one encryption key K1 of the encryption key used for encrypting the data to be transmitted in the isochronous transmission mode and the encryption key used for encrypting the data to

be transmitted in the second transmission mode on the basis of the information indicating the validity of the apparatus itself, the received random number R1 and the generated random number S1, the receiving control means receives data P generated on the basis of the generated encryption key K1, the received random number R2 and the generated random number S2, generates one encryption key K'1 of the encryption key used for decrypting the data transmitted in the isochronous transmission mode and the encryption key used for decrypting the data transmitted in the second transmission mode on the basis of the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, verifies whether or not data P' generated on the basis of the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P. and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the second information processing apparatus and generates the encryption key K'2 of the transmission mode for which the encryption key is not generated yet, of the encryption keys used for decrypting the data transmitted in the isochronous transmission mode and the second transmission mode, on the basis of the encryption key K'1 of the transmission mode for which the encryption key is already generated, the received random number S2 and the generated random number R2.

100. (Previously presented) The first information processing apparatus as claimed in claim 99, wherein the receiving control means generates the encryption key

K'1 on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 on the basis of the result of calculation of a unidirectional function using the generated encryption key K'1, the received random number S2 and the generated random number R2.

101. (Previously presented) The first information processing apparatus as claimed in claim 100, wherein the receiving control means receives data P generated by the second information processing apparatus on the basis of the result of calculation of the unidirectional function using the generated encryption key K1, the received random number R2 and the generated random number S2, verifies whether or not data P' generated on the basis of the result of calculation of the unidirectional function using the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the result of calculation of the unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the second information processing apparatus.



102. (Previously presented) The first information processing apparatus as claimed in claim 100, wherein the receiving control means generates the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function.

103. (Previously presented) The first information processing apparatus as claimed in claim 102, wherein the receiving control means generates the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function.

104. (Previously presented) The first information processing apparatus as claimed in claim 102, wherein the receiving control means generates the encryption key K'1 and the encryption key K'2, using the least significant n bits of the result of calculation of the unidirectional function.

105. (Previously presented) The first information processing apparatus as claimed in claim 104, wherein the receiving control means generates the data Q and the data P' using the most significant m bits of the result of calculation of the unidirectional function.

106. (Previously presented) The first information processing apparatus as claimed in claim 99, wherein the receiving control means generates the encryption key K'1 on the basis of the result of calculation of a unidirectional function with respect to

concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 on the basis of the result of calculation of a unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K'1, the received random number S2 and the generated random number R2.

107. (Previously presented) The first information processing apparatus as claimed in claim 106, wherein the receiving control means receives data P generated by the second information processing apparatus on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K1, the received random number R2 and the generated random number S2, verifies whether or not data P' generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the generated encryption key K'1, the received random number S2 and the generated random number R2 is coincident with the received data P, and in the case where the data P' is coincident with the data P, transmits data Q generated on the basis of the result of calculation of the unidirectional function with respect to concatenated data formed by concatenating the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1 to the second information processing apparatus.